UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/899,293	07/06/2001	Young-Il Kim	P56339	7669

7590 05/15/2007

Robert E. Bushnell
Suite 300
1522 K Street N.W.
Washington, DC 20005-1202

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
05/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/899,293	KIM, YOUNG-IL	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 February 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 22-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 22-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment received February 28, 2007. Claims 1, and 22-28 remain pending consideration.

Response to Arguments

2. Applicant's arguments filed on February 28, 2007 have been fully considered but they are not persuasive for the following reasons:

Regarding claim 1, the Applicant argues that the Cited Prior Art (CPA), Holloway et al. (U.S. Patent 5,805,801) in view of Sofer et al. (U.S. Patent 5,489,896) in further in view of Sherer (U.S. Patent 5,935,245), does not teach "detecting, in the address table, access vectors corresponding to the MAC destination and source addresses." This argument is not found persuasive. Holloway teaches a LAN security feature which reads MAC addresses and using an address table (column 3 lines 15-22, 37-43), checks a list of unauthorized MAC addresses (column 3 lines 37-43). If an unauthorized MAC address is located in the packet, the packet is dropped (column 3 lines 37-43). Therefore, Holloway does teach an access method of denying or granting access based on the MAC address of packets. Furthermore, in a MAC address table with a filter as disclosed by Holloway, the source MAC address is filtered based upon the destination MAC address (certain source MAC addresses are denied access to

certain destination MAC address) (column 8 lines 1-14), wherein in Holloway, certain ports hold certain MAC addresses that users are allowed to access. Though Applicant asserts that no mention of the phrase "access vector" is found, the Examiner has given the term the broadest reasonable interpretation in light of the specification. Claim 1 does not define what an access vector specifically is, and the only cursory discussion, is given in the preamble and not the body of the claim. The Examiner has read the claim in light of the specification, but cannot read the specification into the claim. Therefore, based upon Holloway, the MAC addresses matching, is interpreted as the access control, and the actual though of a "vector" or "bit vector" is taught by Sherer. Sherer and Holloway both involve using rules to filter at the LAN. However, Sherer uses bit vectors to allow or disallow packets (column 6 lines 29-46). This pattern matching used by the bit vectors to allow access (access vectors) expedites the matching process used by the filter of Holloway as the whole packet does not need to be compared and would prevent a spoofing of a MAC address more effectively (column 5 lines 19-23, column 29-34). Based on the broadest reasonable interpretation, the bit vector used for granting or denying access of Sherer is an access vector, and in combination with Holloway-Sofer, teaches access vectors stored in address tables, as the filter of Holloway is in an address table. Furthermore, the Applicant argues that the CPA does not teach, "denying access if the access vectors of the MAC destination and source addresses are not matches." This argument is not found persuasive. The system of Holloway, compares incoming MAC addresses with the destination MAC address, and sees if they are able to communicate based on the filter (column 8 lines 1-14). The

system of Sherer, vectors are compared to see if they adhere to certain rules (column 6 lines 36-40). These rules can be used as an address matching tool such as is implemented by Holloway, and use the vectors to only check a portion of the address (column 29-35). Therefore, in combination, the CPA is respectfully asserted to teach "denying access if the access vectors of the MAC destination and source addresses are not matched." Therefore, the rejection for the claims is maintained as given below for claims 1, and 22-28.

Claim Objections

3. Claims 27-28 are objected to because of the following informalities: Claims 27 and 28 are both claimed as "method claims" and they depend on claim 26, which is an apparatus claims. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, and 22-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Holloway et al. US (5,805,801) in view of Sofer et al. US (5,489,896) in further in view of Sherer (U.S. Patent No. 5,935,245).

As per claim 1: Holloway discloses A MAC (media access control) address based communication restricting method using access vectors stored in address tables, wherein the access vectors indicate whether two nodes, corresponding to a MAC source address and a MAC destination address, may access each other, (Col 3, lines 15-16) the method comprising the steps of:

Receiving packet data upon request of communication through at least one port of a plurality of ports of an Ethernet switch (Column 6, lines 27-30);

Holloway teaches obtaining the destination MAC addresses through the discovery phase (item 145 of FIG. 10 and item 131 of FIG 11) but Holloway does not explicitly teach Reading a MAC destination address and a MAC source address included in the received packet data. However Sofer discloses a MAC address-based communication access control method (Col 3, lines 49-52). Where he teaches the using of a MAC address stripper to extract the source and destination MAC addresses from a packet Col 4, lines 13-22). Therefore, it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Holloway's invention with the teachings of Sofer to include a MAC stripper to extract the MAC destination and source addresses from the received packets. One would be motivated to do so in order to provide the system with ability to determine where did the packet come form and where the packet is headed to and if it's headed to a protected destination. Detecting In an address table, access vectors corresponding to the MAC destination and source address (FIG 6 and Col 9, Lines 49-51 with Col 3, lines 7-9). Holloway teaches using

combination of data structures AAL (access authorization List) and ICD (interconnected device list) the ICD will contain information on connected MAC addresses to the specific Managed hub while the AAL will contain the security access control information for each device. The combination of those two will perform the same function as the address table) which is denying access if the access vectors of the MAC destination and source addresses are not matched (Col 3, Lines 9-11; if the managed hub detects an unauthorized station connecting to the LAN the hub disables the port disabling the port on the hub will perform the step of denying access).

Holloway-Sofer does not disclose that the access vectors are "bit vectors" which are used to allow or disallow forwarding to a destination address. Sherer discloses a MAC security method which uses Value Bit Vectors and Don't Care Bit Vectors to allown or disallow incoming packets (column 6 lines 29-46). These bit vectors are used in a comparison mechanism which compare the values stored in the vectors, and if verified, the packet reception and forwarding is allowed, and otherwise, the packet is discarded (column 6 lines 30-46). It would have been obvious to use the bit vectors of the Sherer invention, to improve security in a LAN by using pattern matching, and allows verification to take place at anywhere in the packet by using the bit vector (Sherer: column 7 lines 12-25).

As per claim 22: Holloway discloses a packet switch communication method, comprising the steps of:

receiving packet data upon request of communication through at least one port of a plurality of ports of said packet switch (Column 6, lines 27-30);

determining whether said received MAC source address is stored in an address table having an access vector indicating whether allowance for access of client nodes is made or not, wherein each client node is identified by at least corresponding MAC address (item 132 of FIG 11 and Column 11 lines 14-16);

when it is determined that said MAC source address is stored in said address table, determining whether an access vector corresponding to said received MAC destination address is matched with an access vector corresponding to said received MAC source address, wherein both of the access vectors are stored in said address table (Column 11, lines 46-50);

if the access vectors corresponding to said received MAC destination and source addresses are matched, transmitting said received packet data to a MAC destination address (Column 3, Lines 9-11); and

denying access if said access vectors of said received MAC destination and source addresses are not matched (Col 3, Lines 9-11; if the managed hub detects an unauthorized station connecting to the LAN the hub disables the port disabling the port on the hub will perform the step of denying access).

Holloway teaches obtaining the destination MAC addresses through the discovery phase (item 145 of FIG. 10 and item 131 of FIG 11) but Holloway does not explicitly teach reading a MAC destination address and a MAC source address included in the received packet data. However Sofer discloses a MAC address-based

communication access control method (Col 3, lines 49-52). Where he teaches the using of a MAC address stripper to extract the source and destination MAC addresses from a packet Col 4, lines 13-22). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Holloway's invention with the teachings of Sofer to include a MAC stripper to extract the MAC destination and source addresses from the received packets. One would be motivated to do so in order to provide the system with ability to determine where did the packet come form and where the packet is headed to and if it's headed to a protected destination. Detecting In an address table, access vectors corresponding to the MAC destination and source address (FIG 6 and Col 9, Lines 49-51 with Col 3, lines 7-9). Holloway teaches using combination of data structures AAL (access authorization List) and ICD (interconnected device list) the ICD will contain information on connected MAC addresses to the specific Managed hub while the AAL will contain the security access control information for each device. The combination of those two will perform the same function as the address table) Denying access if the access vectors of the MAC destination and source addresses are not matched (Col 3, Lines 9-11; if the managed hub detects an unauthorized station connecting to the LAN the hub disables the port disabling the port on the hub will perform the step of denying access).

Holloway-Sofer does not disclose that the access vectors are "bit vectors" which are used to allow or disallow forwarding to a destination address. Sherer discloses a MAC security method which uses Value Bit Vectors and Don't Care Bit Vectors to allown or disallow incoming packets (column 6 lines 29-46). These bit vectors are used

in a comparison mechanism which compare the values stored in the vectors, and if verified, the packet reception and forwarding is allowed, and otherwise, the packet is discarded (column 6 lines 30-46). It would have been obvious to use the bit vectors of the Sherer invention, to improve security in a LAN by using pattern matching, and allows verification to take place at anywhere in the packet by using the bit vector (Sherer: column 7 lines 12-25).

As per claim 23: Holloway discloses the method as set forth in claim 22, further comprising the steps of:

configuring an anti-hacker table comprising information pertaining to a plurality of the client nodes and a plurality of server nodes of a network, wherein each server node is identified by at least a corresponding MAC address (Col 7, Lines 7-13 and FIG 7);

when it is determined that said received MAC source address is not stored in said address table, determining whether information corresponding to said received MAC source address is stored in said anti-hacker table (item 135 of *FIG 11, Col 11* lines 21-29, item 137 of *FIG 11* and Col 11 lines 31-34); and

when it is determined that said received MAC source address is stored in said anti-hacker table, modifying an access vector in said MAC source address to a security key, to thereby store the modified address in said address table (item 320 of FIG 13 and Col 13 lines 34-36 / setting the filter in Holloway system perform the task of setting security by defning which MAC addresses are allowed or denied access to the destination MAC addresses).

As per claim 24: Holloway discloses the method as set forth in claim 23, further comprising the steps of:

adding a port number, corresponding to the port through which said packet data was received, to a storage area corresponding to said MAC source address received in said anti-hacker table (item 265 of FIG 12 and Col 12 lines 17-20).

As per claim 25: Holloway discloses a packet switch communication method, comprising the steps of:

receiving packet data upon request of communication through at least one port of a plurality of ports of said packet switch (Col 6, lines 27-30);

determining whether said received MAC source address is stored in an address table having an access vector indicating whether allowance for access of client nodes is made or not, wherein each client node is identified by at least corresponding MAC address (item 132 of FIG 11 and Col 11 lines 14-16);

when it is determined that said received MAC source address is not stored in said address table determining whether information corresponding to said received MAC source address is stored in said anti-hacker table (item 220 of *FIG* 12 and Col 11, lines 62-64); and

when it is determined that said received MAC source address is stored in an anti-hacker table, modifying an access vector in said MAC source address to a security key, to thereby store the modified address in the said address table, said anti-hacker table

comprising information pertaining to a plurality of said client nodes and a plurality of server nodes of a network, wherein each server node is identified by at least corresponding MAC address (item 320 of FIG 13 and Col 13 lines 34-36 / setting the filter in Holloway system perform the task of setting security by defining which MAC addresses are allowed or denied access to the destination MAC addresses).

Holloway teaches obtaining the destination MAC addresses through the discovery phase (item 145 of FIG. 10 and item 131 of FIG 11) but Holloway doesn't explicitly teach Reading a MAC destination address and a MAC source address included in the received packet data. However Sofer discloses a MAC address-based communication access control method (Col 3, lines 49-52). Where he teaches the using of a MAC address stripper to extract the source and destination MAC addresses from a packet Col 4, lines 13-22). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Holloway's invention with the teachings of Sofer to include a MAC stripper to extract the MAC destination and source addresses from the received packets. One would be motivated to do so in order to provide the system with ability to determine where did the packet come form and where the packet is headed to and if it's headed to a protected destination. Detecting In an address table, access vectors corresponding to the MAC destination and source address (FIG 6 and Col 9, Lines 49-51 with Col 3, lines 7-9). Holloway teaches using combination of data structures AAL (access authorization List) and ICD (interconnected device list) the ICD will contain information on connected MAC addresses to the specific

Managed hub while the AAL will contain the security access control information for each device. The combination of those two will perform the same function as the address table) Denying access if the access vectors of the MAC destination and source addresses are not matched (Col 3, Lines 9-11; if the managed hub detects an unauthorized station connecting to the LAN the hub disables the port disabling the port on the hub will perform the step of denying access).

Holloway-Sofer does not disclose that the access vectors are "bit vectors" which are used to allow or disallow forwarding to a destination address. Sherer discloses a MAC security method which uses Value Bit Vectors and Don't Care Bit Vectors to allown or disallow incoming packets (column 6 lines 29-46). These bit vectors are used in a comparison mechanism, which compare the values stored in the vectors, and if verified, the packet reception and forwarding is allowed, and otherwise, the packet is discarded (column 6 lines 30-46). It would have been obvious to use the bit vectors of the Sherer invention, to improve security in a LAN by using pattern matching, and allows verification to take place at anywhere in the packet by using the bit vector (Sherer: column 7 lines 12-25).

As per claim 26: Holloway discloses a MAC (media access control) address-based communication restricting packet switch comprising:

a plurality of MAC ports (Col 4, lines 67 through Col 5, lines line 1);

a data exchange for establishing paths of packet data between MAC ports;

a packet memory storing an address table having access vector indicating whether allowance for access of client nodes is made or not, wherein each client node is identified by at least corresponding MAC address (FIG 6 and Col 9, Lines 49-51 with Col 3, lines 7-9) said port table storing information about a current status of the packet switch, port attributes and enable/disable, and packet reception completion of each MAC port (Col 11, lines 44-50) and said address table storing registered MAC addresses, destination access vectors corresponding to destination MAC addresses of said registered MAC addresses (FIG 6 and Col 9, Lines 49-51 with Col 3, lines 7-9);

a transmission/reception controller controlling data exchange (Col 5, lines 2-12);

wherein said transmission/reception transmits said received packet data to a MAC destination address when said received MAC source address is stored in said address table and if an access vector corresponding to said received MAC source address is matched with an access vector corresponding to said received MAC source address (Col 3, Lines 9-11),

denies access if said access vectors of said received MAC destination and source addresses do not match (Col 3, Lines 9-11; if the managed hub detects an unauthorized station connecting to the LAN the hub disables the port disabling the port on the hub will perform the step of denying access).

Holloway does not disclose that the access vectors are "bit vectors" which are used to allow or disallow forwarding to a destination address. Sherer discloses a MAC security method which uses Value Bit Vectors and Don't Care Bit Vectors to allown or disallow incoming packets (column 6 lines 29-46). These bit vectors are used in a

comparison mechanism which compare the values stored in the vectors, and if verified, the packet reception and forwarding is allowed, and otherwise, the packet is discarded (column 6 lines 30-46). It would have been obvious to use the bit vectors of the Sherer invention, to improve security in a LAN by using pattern matching, and allows verification to take place at anywhere in the packet by using the bit vector (Sherer: column 7 lines 12-25).

As per claim 27: Holloway discloses a MAC address-based communication restricting packet switch communication method as set forth in claim 26,

when said received MAC source address is not stored in the address table, and if information corresponding to the received MAC source address is stored in an anti-hacker table, modifying an access vector in said MAC source address to a security key, to thereby store the modified address in the said address table, wherein said anti-hacker table comprises information pertaining to a plurality of client nodes and a plurality of server nodes, wherein each server node is identified by at least corresponding MAC address (item 320 of FIG 13 and Col 13 lines 34-36 / setting the filter in Holloway system perform the task of setting security by defining which MAC addresses are allowed or denied access to the destination MAC addresses).

As per claim 28: Holloway discloses a MAC address-based communication restricting packet switch communication method as set forth in claim 27, wherein said

transmission/reception controller adds a port number, corresponding to the MAC port through which said data packet was received, to a storage area corresponding to said received MAC source address in said anti-hacker table (item 265 of FIG 12 and Col 12 lines 17-20).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA K.A.
05/09/2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100